September 1992/Number 4-92

security awareness bulletin

Inside:

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

Staff Writer
Tracy Gulledge

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Educational Programs Department, c/o Defense General Supply Center, Richmond Virginia 23297-5091; (804) 279-3824/4223, DSN 695-3824/4223. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods as well as through distribution of textual material for direct training application.

Administrative inquiries, new distribution, address changes: please refer as follows:

Army activities: HQ DA (DAMI-CIS), Washington, DC 20310, (202) 695-8920, DSN 225-8920; POC Jim McElroy

Navy & Marine Corps: Security Policy Div (OP-09N), Washington, DC 20350 (202) 433-8855. DSN 288-8855; POC Sue Jones

Air Force: Headquarters AFSPA/SPGB, Kirtland AFB, NM 87117, DSN 246-4787; POC MSgt. Mike Trammel

DIS activities: HQ DIS/V0953, 1900 Half St SW, Washington DC 20324-1700

DISP contractors: Cognizant Security Office

Other government agencies: Headquarters security education office

What is the Threat and the New Strategy?

by David G. Major
Special Assistant to the Assistant Director in Charge, Intelligence Division, Federal Bureau of Investigation

The collapse of international communism, the democratization of Eastern Europe, and the dismemberment of the former Soviet Union have forced us to dramatically reinterpret the international intelligence threat to the United States. Those who can speak for the intelligence community have been understandably cautious about making authoritative pronouncements about who is threatening us militarily, economically, and politically. Things have been moving so fast that anything but the most general interpretation of events is soon out of date. However, there has been an on-going interagency effort to assess what changes have taken place in the international intelligence arena and what future developments we are likely to see.

Over 50% of the 170 countries in the world conduct intelligence collection operations against the U.S.

A truly international threat

While the line between friendly nations and potential adversaries has blurred, be aware that of the 170-plus countries in the world, over 50% of them conduct some level of intelligence collection operations against the U.S. During the Cold War, the U.S. counterintelligence community focused on about 11% of these countries, and we referred to them as the *hostile intelligence threat.*

Historically we were primarily concerned with the Soviet intelligence services--the KGB (Committee for State Security), the GRU (the Chief Intelligence Directorate of the Ministry of Defense), and the assortment of satellite services from Bloc nations which, often with greater success, launched sophisticated human intelligence (HUMINT) operations against U.S. citizens at home and abroad. The big question is, where has this monolithic intelligence empire gone? The former Soviet services are undergoing rapid evolution in terms of function and geographic scope. They are, however, still alive and well. The infrastructure of the KGB remains and still has the same mission for external collection activities.

Demise of the old KGB?

The former 1st Chief Directorate of the KGB is now the Russian Foreign Intelligence Service (SVRR). The old KGB was a big loser in the coup attempt, but the axes fell on top management. The middle management and "worker bee" infrastructure is still intact. They have not stopped or even slowed their operations. The Russians are still meeting and paying their agents. We believe the Russians are being more cautious in their operations to avoid potential political embarrassment, and therefore stress quality of collection rather than quantity.

The KGB SIGINT (and other technical collection) apparatus simply changed its name and has continued its operation with no observable changes in level or methods. The GRU (military intelligence) is still very much in the collection business. There have been no indications that their efforts have decreased in intensity. They are still accepting volunteers and meeting with agents worldwide.

Former satellite intelligence services

Significant changes, however, have occurred in Eastern Europe. Five countries formerly in the Soviet Bloc have shut down their collection activities against the U.S.:

- East Germany no longer exists. Revelations from the intelligence files of the former German Democratic Republic show that East German in-

The infrastructure of the KGB remains and still has the same mission for external collection activities.

telligence was very successful. Their success is not surprising when you consider that they had more than 80,000 professional intelligence officers and almost 1 million non-professional agents and informants in a nation of 18 million individuals.

- Poland is no longer running collection operations against the U.S. and has withdrawn intelligence officers from North America.
- Hungary has terminated operations against us.
- Czechoslovakia fired and replaced its *entire* intelligence apparatus. Their operations against the United States have terminated.
- Bulgaria has also stopped its collection efforts targeting the United States.

The much-publicized reassignment of 300 FBI agents from counterintelligence to other missions was done in response to the disappearance of the threat from the five countries listed above. It indicates that we do not currently face an intelligence threat from these countries and nothing more.

An exception to the general trend of other Central European countries is Rumania, whose intentions regarding collecting against the U.S. are unclear. There are some indications that they may be increasing their efforts, and are therefore still considered a threat.

Shifting our attention to the non-traditional threat

The changes in the threat from Eastern Europe and the old Soviet camp have allowed us to also focus our attention on the "non-traditional threat"—the threat from the remaining "50%" that actively target the United States. This is actually not a new threat, but a new recognition or acceptance of what the intelligence community has been saying for some time: there may be friendly nations, but few friendly foreign intelligence services.

What we are calling the non-traditional threat includes many members of the Third World which have targeted U.S. citizens working overseas. The most well-known example of this is Ghana which successfully coopted a U.S. diplomatic employee several years ago.

There are also nations which are interested in nuclear, chemical, or biological proliferation. Iraq and other countries use their intelligence services to assist in the development of these capabilities. This category includes our allies which do not have benign intelligence services with regard to our companies and technology.

Domestic volunteers: a continuing problem

One thing to keep in mind is that the changes in international politics have nothing to do with the motivations of the "volunteer agent." These include people (U.S. citizens) like John Walker, Ronald Pelton, and more recently, Jeffrey Carney. Since these individuals appear to be motivated by many factors including a need for money, revenge, or by more deep-seated psychological causes, the collapse of international communism has little or no significance to them. People intent on betrayal of a trust, for whatever reason, will look for other customers. Needless to say, a top priority in our counterintelligence strategy is to identify and deal with these "volunteers" before they can damage national interests.

A new strategy for combatting the threat

Because of these dramatic changes in the nature of the threat, the FBI has adopted a new counterintelligence strategy which has been in effect since February 1st, 1992. This strategy is based on a number of assumptions. First, the number of foreign intelligence services targeting U.S. information is not likely to decrease. Second, national security and economic strength are indivisible, and as a corollary, economic and military strength depend on both our intelligence collection efforts and effective counterintelligence. Third, our counterintelligence organizations must be responsive to change and serve as an alarm bell to the larger community.

We cannot overlook a couple of facts of life that have made our job more difficult and have led us to reexamine the way in which we allocate limited resources to meet the new threat: (a) the massive influx of foreign nationals from the former Soviet

There may be friendly nations, but few friendly foreign intelligence services.

The number of arrests for espionage is* not *a reflection of the level of foreign intelligence collection activities directed at U.S. interests.

Union and Bloc nations—both visitors and commercial representatives—to the United States, and (b) the corresponding increase of U.S. citizens travelling to formerly restricted areas for business and pleasure.

The National Security Threat List

Consequently, no longer will the Bureau focus on a set of "hostile countries." Instead of a "country list," there will be a two-part "National Security Threat List" (the NSTL) which will be reviewed and updated annually.

U.S. intelligence agencies will continue to identify countries or other political entities which can be expected to mount collection operations against us. These will be reviewed by the FBI and Department of Justice in cooperation with the State Department. Inclusion on the list will be based on the observed level of intelligence activity; the nature of the information being targeted; the capability of that country or entity to conduct intelligence activities; and our political, military, and economic alignment with that country. The nations or political entities identified as threats under the NSTL will be classified. This part of the list will not be disseminated outside of the FBI since it is an internal mechanism for directing the Bureau's foreign counterintelligence operations. However, defense contractors and Federal agencies will continue to be alerted about specific threat situations through the DECA program (Development of Espionage and Counterintelligence Awareness) and other special briefings.

The second part of the list identifies issues critical to our national security. Some of these issues include: national defense information, critical technology, economic proprietary information which affects our industrial base, and foreign policy information. Some of these categories of information clearly fall outside of the realm of traditionally classified information. (Editor's note: see the chart that follows.) The objectives of the NSTL will be to identify and neutralize the foreign intelligence threat, focus on the collector and its targets, identify the nation's most precious secrets, and focus and direct CI investigations against intelligence activities.

I wish to stress that the prosecution of "spies", while paramount in our counterintelligence program, is not the only possible response to the discovery and interdiction of intelligence collection efforts. In fact, fewer than ten percent of the clandestine agents we identify are ever prosecuted. Among the numerous reasons why agents might not be arrested or prosecuted are: It may be to our advantage to (a) exploit specific operations to learn the methods, techniques, and structures of intelligence services or (b) to mount a double-agent operation against the source. What is important to recognize is that the number of arrests for espionage is *not* a reflection of the level of foreign intelligence collection activities directed at U.S. interests. Each year we arrest and prosecute only a handful of those individuals involved in espionage as compared to the hundreds of espionage operations which we actually neutralize.

Bottom Line for the NSTL

An offensive CI response will be directed against *any* foreign power conducting intelligence activities against the U.S. regardless of our political, military, or economic alignment with that country. Our strategy will be flexible, sensitive, and responsive not only to rapid changes in the geopolitical world stage, but also to the growth of new technologies and to intelligence operations launched by friend and foe alike which target U.S. interests.

National Security Threat List Issue Threats

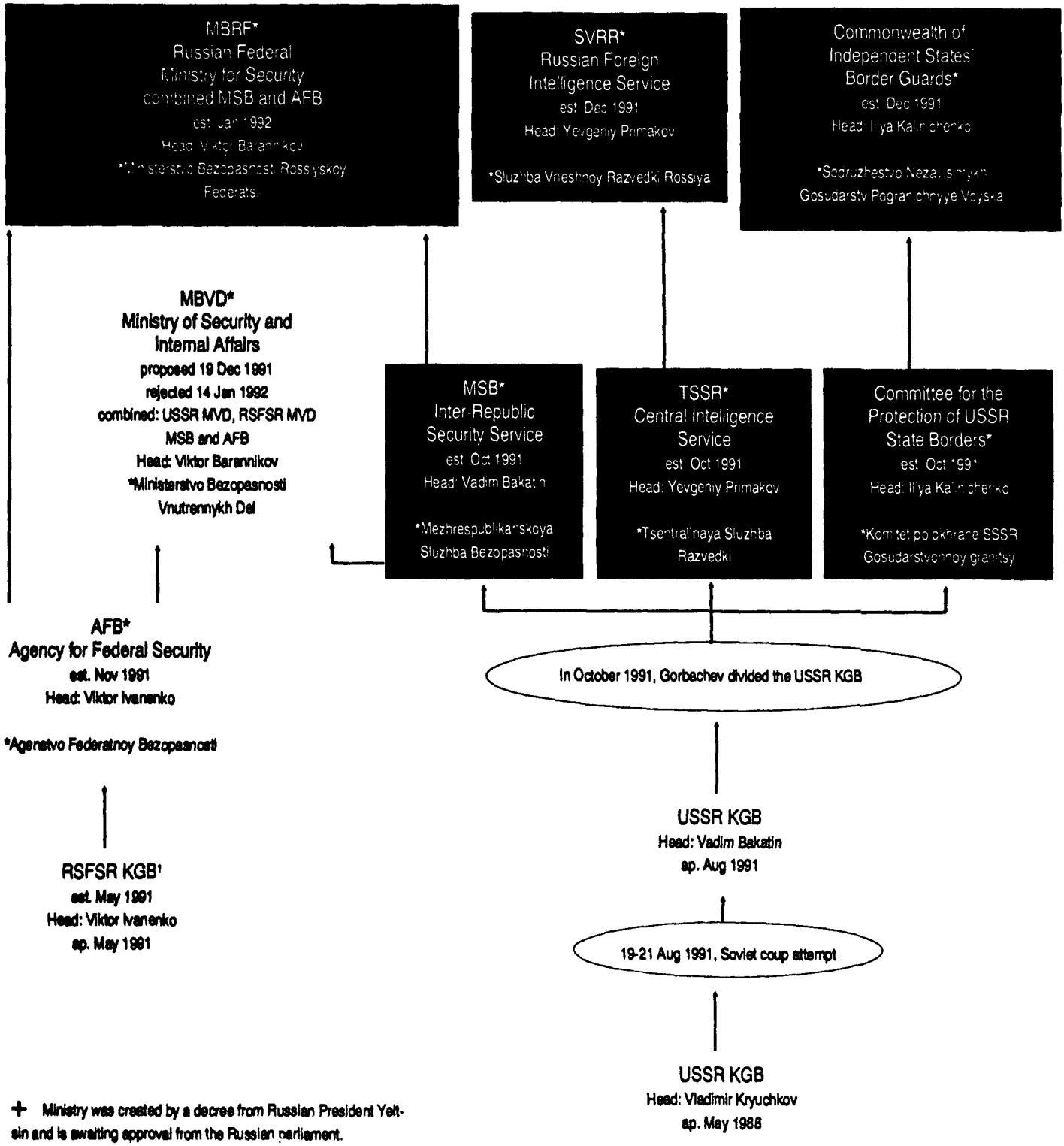
The following categories of activities designated as issue threats under the NSTL as of December 30, 1991:

- Foreign intelligence activities directed at United States critical technologies as identified by the National Critical Technologies Panel[1]
- Foreign intelligence activities directed at the collection of United States industrial proprietary economic information and technology, the loss of which would undermine the U.S. strategic industrial position
- Clandestine foreign intelligence activity in the United States
- Foreign intelligence activities directed at the collection of information relating to defense establishments and related activities of national preparedness
- Foreign intelligence activities involved in the proliferation of special weapons of mass destruction or delivery systems of weapons of mass destruction
- Foreign intelligence activities involving the targeting of U.S. intelligence and foreign affairs information and U.S. government officials
- Foreign intelligence activities involving active measures[2]

[1] *The National Critical Technologies Panel, established in FY 1990, is charged with identifying up to 30 technologies essential for our long-term national security and economic prosperity. It consists of 13 members with expertise in the fields of science and engineering chosen from the Federal government and the private sector.*

[2] *propaganda and disinformation programs by foreign intelligence services to discredit the United States*

Evolution of the Russian Intelligence Services



+ Ministry was created by a decree from Russian President Yeltsin and is awaiting approval from the Russian parliament.

[1] Russian Soviet Federal Socialist Republic

March 1992

WOW!!! Something New!!!

COURSE TITLE

Personnel Security Interview Course
(5220.15)

LOCATION

Department of Defense Security Institute
c/o Defense General Supply Center
Richmond, Virginia 23297-5091

LENGTH

Three and One-Half Days

PURPOSE

The *Personnel Security Interview Course* is designed to train and educate DoD personnel who conduct interviews of individuals who perform sensitive duties or work in a security environment.

SCOPE

The *Personnel Security Interview Course* offers training in how to properly conduct a subject interview. Lessons address the purpose of the interview; how to prepare for the interview; the procedures for controlling and conducting interviews; appropriate and inappropriate areas of questioning; effective listening; and how to identify, follow up and resolve issues raised by the interview. The *Personnel Security Interview Course* uses extensive practical exercises, providing students with several opportunities to apply the knowledge and skills taught. Some outside-of-class preparations and problem-solving assignments are required.

PREREQUISITES

This course is for DoD civilian, military or contractor personnel who conduct personnel security interviews. Personnel from other federal agencies are eligible to attend on a space available basis.

ACADEMIC REQUIREMENTS

Regular attendance at and participation in all sessions is required for a certificate of completion.

Don't confuse this course with the Basic Personnel Security Investigations Course (BPSIC). If your employees conduct personnel security investigations, you want BPSIC. But if they conduct pre-investigative interviews to screen personnel, or post-adjudicative interviews to resolve issues, the *Personnel Security Interview Course* is for you.

TRAINING FUNDS A PROBLEM?

If so, it might make sense to host an offering of the *Personnel Security Interview Course* at your location (even overseas). If you provide the facilities, your only cost would be the TDY expenses of 2-3 DoDSI instructors. In addition, we would be willing to tailor the course content and practical exercises to meet your specific needs and your agency's policies. For more information, call DoDSI at DSN 695-4891 or 804-279-4891.

Origin And History Of The National Industrial Security Program

By Maynard Anderson
Assistant Deputy Under Secretary of Defense
(Security Policy)

Background

The National Industrial Security Program (NISP) is a single, coherent, and integrated government security program with uniform, consistent standards and procedures for the protection of government classified information held by industry. It mandates that all government departments and agencies which contract with private companies to perform work requiring the use of government classified information will protect that information in a uniform way and in accordance with a single government regulation.

Events leading to creation of a NISP took form as identifiable activities in the early 1980's when various government and industry security officials began to express concerns about the process and effectiveness of safeguarding classified information held by industry. The concerns grew out of the increasing number of separate, conflicting, confusing and sometimes arcane regulations prepared by each government department and agency or the protection of the same kinds of information. Documentation of circumstances began to emerge in which classified information was subjected to indiscriminate, inconsistent, repetitious, unnecessary, and even unworkable, security procedures at costs not commensurate with the risk of compromise. Informal discussions of the evolution of these situations among industry and government officials over a period of years had resulted in no significant progress toward improvement.

Because of the predominance of the Defense Industrial Security Program (DISP) in industrial contracting by the government, the Department of Defense (DoD) was clearly responsible for many of the situations and actions that led to the NISP concept. During the late 1970's and early 1980's there began to emerge a specter that concerned the Director, Defense Investigative Service (DIS), as the administrator of the DISP. His concerns centered around the emergence of numerous special access programs (SAPs) protecting weapon system acquisition, many of which had diverse requirements and were "carved out" from inspection by the DIS. Some of these SAPs were created by renegade program managers who believed that they allowed more efficient operations. In fact, they imposed costly requirements on the contractors involved and hid from view possible security irregularities that would have been disclosed through regular, impartial inspections.

In all fairness, some of these programs that controlled advanced technologies used to produce modern, sophisticated weapon systems were of benefit to the government. They were outnumbered, however, by those of questionable value that appeared to be nothing more than a means to circumvent proper inspections and, sometimes, proper management.

Special access programs may be created only by designated Agency Heads pursuant to Section 4.2 of Executive Order 12356, "National Security Information," April 6, 1982.

The criteria for establishment of SAPs are, (a) normal management and safeguarding procedures do not limit access sufficiently to the nation's most sensitive national security information, and (b) the number of persons with access is limited to the minimum number necessary to meet the objectives of providing extra protection for the information.

As defined by DoD Directive 0-5205.7, "Special Access Program (SAP) Policy," January 4, 1989, a SAP is, "Under the authority of E.O. 12356 ... and as implemented by the ISOO Directive No. 1 ... any program created by an Agency Head whom the President has designated in the Federal Register to be an original TOP SECRET classification authority that imposes "need-to-know" or access controls beyond those normally required by DoD Regulations for access to CONFIDENTIAL, SECRET, or TOP SECRET information." Prior to issuance of this directive, SAP creation and oversight in the DoD was controlled inconsistently.

This article is an edited version of Mr. Anderson's paper: "A Prudent Approach to Industrial Security—The National Industrial Security Program."

The Harper Committee Report was a report to the Deputy Under Secretary of Defense for Policy by the Department of Defense Industrial Security Review Committee (December 1984) which contained an analysis of the effectiveness of the DoD Industrial Security Program and offered recommendations for program improvement. The committee was convened as a result of the arrest of James Durward Harper, Jr., for alleged espionage activity involving a DoD contractor facility, and it was from him that it obtained its name.

In counterpoint, the DIS administration of the program was accused of having become so structured, rigid, and inflexible that many program managers sought relief in provisions that allowed them to be exempt from regulations of the DISP.

Reports continued to circulate of large numbers of government inspectors visiting the same facilities to look at the same things, and levying ad hoc, sometimes whimsical, requirements on their hosts. As a result, and in the name of security, large amounts of money were spent to build unnecessary facilities, investigate personnel for high clearances and accesses of questionable need, and control information that was protected beyond its sensitivity.

There had been little support from any quarter for changes to industrial security policies or procedures to this point. Much discussion, and some hand-wringing continued over a state of affairs that was recognized as problematic, but progress toward improvement was not discernible.

Disunity existed within both government and industry as to what action could be taken, or how action might be taken to relieve the affects on contractors of rigid and dogmatic enforcement of industrial security procedures on the one hand, and ad hoc requirements of multiple customers on the other hand. Some officials were loathe to act because the status quo was their desirable condition. Others felt that everything was all right and, "if it ain't broke, don't fix it." Some wanted to abolish all SAPs as unnecessary, excessive, and costly. Some wanted to "reform" the industrial security programs, generally. And, there were those in industry who believed that taking the initiative to offer program improvements would result in prejudicial criticism of their efforts, or even vindictive retribution against their firms or organizations by government officials with authority over the programs concerned.

Slowly, during the mid-1980's, industry began to become more involved in industrial security policy formulation. Representatives of industry participated in both the Harper Committee and the Stilwell Commission. Representatives of industry began independently to formulate positions that would lead to a single industrial security program.

With the encouragement and support of several key government officials, industry representatives intensified their efforts and between March and July 1988, generated several iterations of a "white paper" entitled, "Toward a Rational Industrial Security Program." Despite the lack of wide-spread government support, industry representatives were encouraged to document and develop supporting data for changes and to outline their ideals for a consolidated program.

On the basis of preliminary but unconfirmed data, industry began to build a plan for a single program and documented the number of conflicting and overlapping policies and redundancies while identifying associated costs for all security disciplines and programs.

Concept Development

In March 1988, under the auspices of the Aerospace Industries Association (AIA) Industrial Security Executive Committee, security officials from a number of leading defense contractors and the government began working together, but informally, on a program to standardize security practices within industry. The Industrial Security Committee of AIA approved continued project development. It was recognized that continuing top-level

The Stilwell Commission, named in honor of its chairman, General Richard G. Stilwell, USA (Retired)(1917-1991), was established by the Secretary of Defense as the DoD Security Review Commission in the wake of arrests of three retired and one active duty Navy member on charges of espionage. The Commission was directed to conduct a review and evaluation of DoD security policies and procedures and identify any systematic vulnerabilities or weaknesses in the programs. It produced a report on 19 November 1985, "Keeping the Nation's Secrets."

government and industry support was critical to the success of the initiative. As earlier efforts to "work within the system" had failed, AIA executives along with other industry officials introduced the concept with a "top down" approach to Chief Executive Officers (CEOs) and senior government activities.

During an AIA Industrial Security Committee meeting in May 1988, there had been extensive discussion concerning the possible form and substance of something like a National Industrial Security Program (NISP). Suggestions were advanced that the NISP should be codified in federal law, something that had been attempted during the late 1960's without success. It was understood, too, that if the program were established by law, it could only be changed or modified by amendments to the law, a situation which would probably result in an unacceptably inflexible program. Conferees generally agreed that an Executive Order would probably be the most practical instrument of authority.

On 26 July 1988, AIA representatives presented the details of a proposed NISP concept and strategies to the Assistant Deputy Under Secretary of Defense (Counterintelligence and Security) and the Director, Defense Investigative Service. Support and assistance to industry were offered along with encouragement to continue concept development.

In August 1988, AIA sought involvement by the American Society for Industrial Security (ASIS) which committed active assistance. The National Classification Management Society (NCMS) and the National Security Industrial Association (NSIA) also brought support and assistance to the NISP initiative. Industry representatives began to accumulate data acquired through a survey of a limited number of member companies which provided evidence that security policies and procedural requirements generated independently by individual government departments significantly increased costs without improving security.

To further support the belief that the problems identified in the earlier survey were not isolated, AIA conducted an expanded survey of some of the major aerospace companies to determine whether the security issues the NISP concept addressed were valid on a broader scale.

Fourteen companies which derived a total of $32.8 billion annually from government contracts responded to the survey. The fourteen companies employed a total of 340,000 cleared people and had almost twelve million classified documents, fifty-two percent of which were accountable.[1] This was a sizable survey to counter arguments of isolated problems and to gain support for more cost-effective security.

Five elements of existing industrial security programs were highlighted in industry's survey: Personnel Security; Security Briefings; Security Inspections; Physical Security; and Automated Information Security (hardware, software, facilities, and manpower).

Industry's total reported cost from this survey was $.8 billion. It projected a $2 to $3 billion cost avoidance if duplication and redundancy with no added security protection could be eliminated through establishment of a single industrial security program.

The survey highlighted a growing need for a consolidated program. It was a turning point in terms of gaining the attention, influence, and support from essential components of the government. Difficulty arose, however, when it became clear that such a program would mean giving up long-standing, traditional, and parochial practices. The need for standardized briefings, inspections, and universally-accepted performance standards for industry were undeniable, but their achievement remained questionable. It would require each government department and agency to accept each other's investigations, accreditations, and inspections, based on the same standards. Some government agencies still held to the ideas that their programs were the best and were working well.

The survey statistics, coupled with a diminishing funding stream, caused support in government circles to grow. From late 1988 until January 1990, AIA zealously kept up the pressure and continued to brief government officials within DoD, the State Department, the Central Intelligence Agency (CIA), the Department of Energy (DoE), the Federal Bureau of Investigation, and others. Government officials expressed enthusiasm with encouragement and many offered their support. A

[1] "Accountable" generally refers to that information classified SECRET and above controlled by a system of records that assures the documentation and tracking of the information in whatever media.

briefing was held for Lt. Gen. Brent Scowcroft, USAF (Retired), Assistant to the President for National Security Affairs in November 1989. He recited personal frustrations resulting from having repeatedly to complete investigative forms despite his long years in the service of his country and the number of previous investigations he had undergone. He commented favorably on the merits of such a program and challenged industry to continue briefing the concept to key government executives.

In December 1989, shortly after the briefing of General Scowcroft, Dr. Robert Gates, then Assistant to the President and Deputy for National Security Affairs, requested that other members of the NSC be briefed on the concept.

By early 1990, most government executives in Washington in a position to influence and create change in government programs had been briefed. Briefings, speeches, symposia involving industry and government representatives, all extolling the virtues of a NISP, intensified in noise and number.

In March 1990, General Scowcroft and Dr. Gates both corresponded with the President of AIA expressing appreciation for industry's efforts concerning the NISP. Lieutenant General Scowcroft noted that "...codifying industrial security procedures under a NISP are of vital importance...We continue to have the concept under active consideration within the Government." Dr. Gates noted, "the NISP concept is an excellent example of what can be accomplished if industry and government work together on problems of mutual interest."

The President Acts

Industry had provided documentation to support its position on the need for a NISP and a government review was now required formally to develop information on the issue.

On 4 April 1990, President Bush signed a National Security Review entitled, "The National Industrial Security Program," in which he directed a review of the government's industrial security programs to determine the feasibility of establishing a single program applicable to all government departments and agencies. He further directed the Secretary of Defense to take the lead and coordinate efforts with the Secretary of Energy and the Director of Central Intelligence.

Significant AIA survey findings included:

- Fourteen government agencies imposed 341 security regulations and directives on industry.
- Twelve government agencies conducted multiple inspections at each facility (one contractor reported fifty-five inspections in one year requiring 442 man-days of effort). One contractor reported 150 SAPs each requiring two annual inspections.
- One-third, or 105,400 cleared employees, completed an average of eight sets of investigative forms for six different agencies.
- An equal number of cleared employees (105,400) required an average of seventeen separate security briefings.
- Industry's total reported cost from this survey was $.8 billion. It projected a $2 to $3 billion cost avoidance if duplication and redundancy with no added security protection could be eliminated through establishment of a single industrial security program.

The Government Review—Phase I

The Secretary of Defense delegated responsibility for the NISP review to the Under Secretary of Defense for Policy on 19 April 1990.

Six government agencies (State, Treasury, Energy, the Nuclear Regulatory Commission, the Attorney General/Federal Bureau of Investigation and the Central Intelligence Agency) and 13 DoD agencies participated in the review; industry was kept abreast of developments through continuing coordination among industrial associations and the review coordinator.

A survey questionnaire designed to elicit similar information as that documented by the earlier industry survey, was developed and provided to all government departments and agencies participating in the review. It produced information that convinced many more government officials that changes were needed, as the total costs (both direct and indirect) for industrial security were estimated at $13.8 *billion*.

The President's National Security Review concerning the NISP sought answers to the following questions:

- How can we standardize security training?
- Can we develop uniform inspection compliance standards?
- What single set of baseline standards can we develop applicable to all government agencies and departments?
- Should there be layered security controls?
- What should industry's role be in the NISP?
- What shifts in priorities and resources are needed to effect a NISP?
- What changes are needed to improve security effectiveness and ensure cost efficiency?
- Which agencies and departments should develop standards and procedures and who should have oversight responsibility?

The government survey provided data on the industrial security program that were heretofore unknown or not publicized. For example:

- The government has more then 15,000 cleared contractor facilities employing more than 1.5 million cleared contractor employees.
- Various rules and regulations implement or supplement the basic executive orders and legislation. They include 47 different standards, manuals, and directives that create a significant regulatory burden to industry and government.
- Various agencies sponsor programs designed to maintain threat awareness in industry. Virtually all agencies and departments of government have security awareness training programs, briefings, and materials available for use by their contractors, but they are all poorly utilized.
- A lack of uniform personnel security requirements and reciprocity of investigations throughout the government cause unnecessary costs as a result of redundant investigations and lost time while personnel wait for clearance.
- Special activities (sensitive compartmented information, SAPs, and Energy/Restricted Data (E/RD) and programs should have supplemental controls only if it has been determined that baseline security programs do not provide adequate protection.
- Security oversight of industry is applied inconsistently by government agencies with generally no reciprocity for facility accreditations, certifications or inspections among agencies and departments.
- Most departments and agencies have no mechanism for determining the costs of the industrial security program. Security costs are generally embedded in other program elements. When estimates were provided, they seemed low. There were no means available within the government for validating and separating security costs from other program costs.

The review confirmed the government's use of multiple rules to protect information of the same sensitivity; inconsistent application and enforcement of those rules; and an inability to determine program costs.

The Response to the President

The report to the President[2] following the initial program review indicated that the concept of a national program for security in industry is feasible and desirable. Moreover, the Secretaries of Defense, Energy, Treasury, the DCI, the Attorney General and the Chairman, NRC, all generally supported the concept of a single integrated system of industrial security for classified programs. The report also contained the general consensus of both government and industry representatives that SCI,

[2] A Report to the President by the Secretary of Defense, "The National Industrial Security Program," November 1990.

SAPs, and Energy-unique activities should be subject to supplemental controls.

The report proposed that an Interagency Task Force led by the Secretary of Defense, the DCI, and the Secretary of Energy, with industry participation, design a national industrial security program to be implemented under the general oversight of the Executive Office of the President.

Again, the President Concurs

On 6 December 1990, the President concurred in the plan and directed that a task force develop elements of a NISP as outlined in the report. The President further requested that recommended policy changes be provided to the National Security Council by 1 September 1991.[3]

The Review—Phase II

The Assistant Deputy Under Secretary of Defense (Counterintelligence and Security) was designated the responsible official for leading and directing the effort.[4]

The NISP Interagency Task Force consisting of an executive committee, steering committee, and 10 working groups, was formally established on 22 January 1991. The steering committee was directed to report to an executive committee, members of which had departmental or agency program approval authority for their respective departments. An eleventh working group, the Monitoring and Evaluation Group, was established to serve as the focal point for all activities and to provide support to the steering committee.

The division of labor among the working groups was designed so that each would concentrate on a separate security discipline. In some cases, like that of the Information Security Working Group, it was determined desirable to form sub-groups to deal with the clearly separate areas of SAPs, SCI, and Energy-related programs. It was the consensus of the entire task force that a working group dealing with threat be established to determine not only changing threats as they affect policy formulation, but improved means of communicating the threats to industry.

Working groups comprised of experts from government and industry labored to:

- Conduct a comprehensive regulatory review
- Develop an instrument of authority for a single industrial security program
- Develop uniform standardized security policies
- Establish a mechanism for determining complete industrial security costs, and
- Ensure completion of ongoing personnel security initiatives for a single scope background investigation applicable to all government departments and agencies.

Formation of the working group on Threat, and creation of the Monitoring and Evaluation Working group were two of the first formal examples of the ability of a combined group of government and industry representatives to achieve consensus on issues related to a NISP.

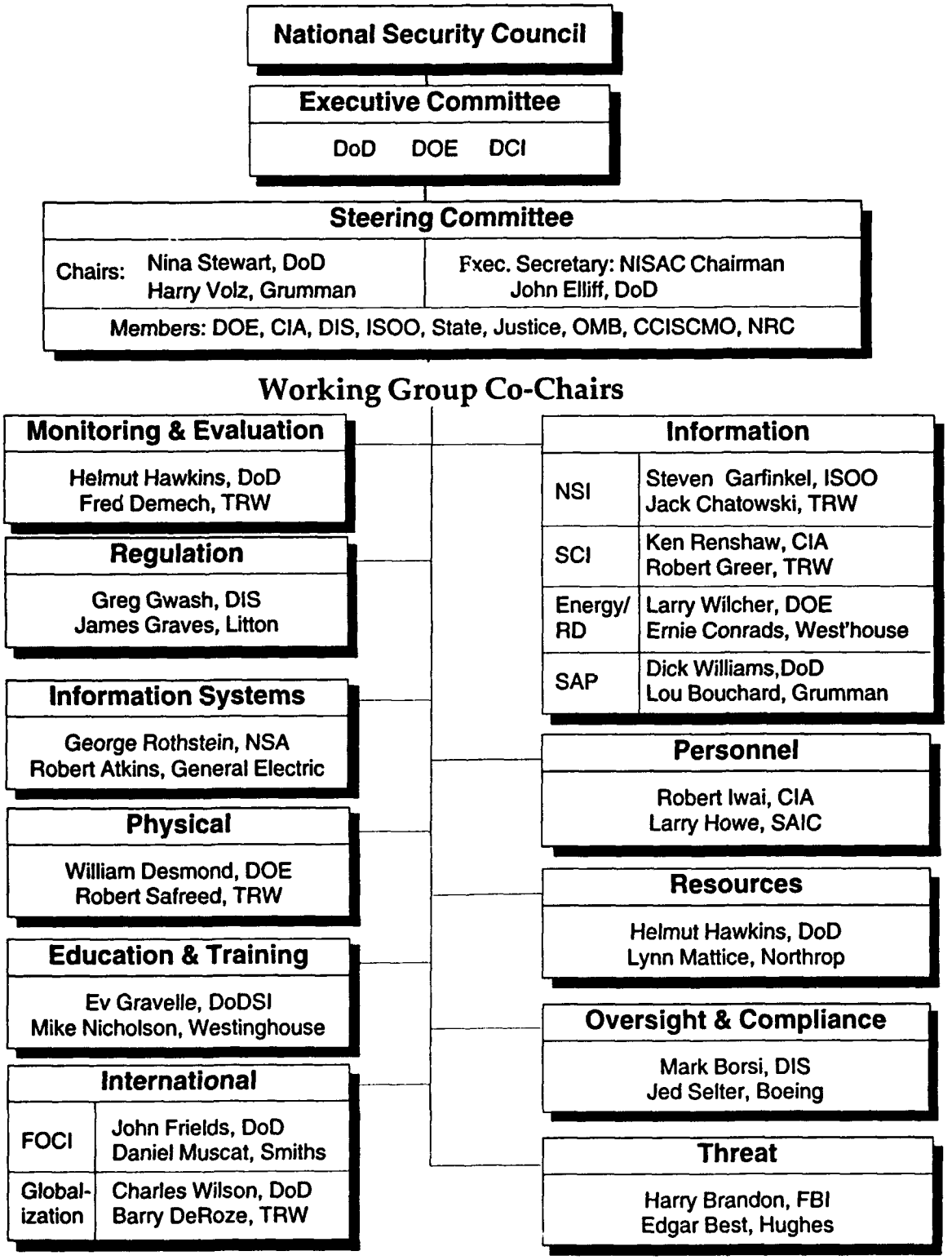
Industry, government, and all affected "communities"[5] were involved in the working groups and the steering committee. Each working group was headed by a government and industry co-chair. The working groups functioned as teams to design the future program elements beginning with basic policies, proceeding to details that would provide the functional guidance to implementers. This concept allowed the formulation of segregable policies, or elements, that could be approved and implemented immediately despite what might happen to the NISP in its entirety. It was decided that each working group would review current policies and procedures, *in toto* and by sub-discipline, respectively, in order to preserve that which works well and which would presumably work well in the future. The preserved elements of current policies and proce-

[3] President's Memorandum to the Secretary of Defense, 6 December 1990.

[4] Based on an organizational change within the Office of the Secretary of Defense, DoD responsibility for the NISP was transferred to the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures) in September 1991.

[5] The term "communities" refers to groups of like organizations, or organizations with related missions and functions, e.g., the Intelligence Community.

Figure 1. National Industrial Security Program Task Force Chart (August 1992)



dures would then serve as the foundation for new innovative elements that would complete the requirements for a program.

An early example of greater efficiency in federal policy-making emerged from the NISP process. A single scope background investigation for access to top secret and SCI had been under consideration in the government for a number of years. When directed by the President, it became an objective of the NISP Task Force also. Agreement concerning its requirements was achieved with relative speed and resulted in a National Security Decision by the President on 21 October 1991. It is also an example of the development of a segregable element of policy.

The working groups were established to deal with discreet security disciplines. A notable exception is the Regulation Working Group which must cross all security disciplines as it works toward its objective of establishing a single regulation. That regulation, to be called the National Industrial Security Program Operating Manual (NISPOM), will include the set of rules by which the NISP will function, along with instructions for both government and industry. Other working groups will feed the Regulations Working Group with the necessary information and material to establish the rules.

Working group chairpersons (a government and industry representative co-chaired each working group) were selected by the steering committee. Chairpersons were responsible for creating their own groups, preparing terms of reference by which to operate, ensuring appropriate representation from government and industry, and for establishing an agenda. The charters and objectives of each group were formalized and submitted to the steering committee for approval.

By late March 1991, most working groups were well into the effort, and on 2 May 1991, the steering committee provided an interim report to the executive committee.[6] The report depicted the task force organization, outlined NISP initiatives, and provided a summary of accomplishments. The report confirmed support by all committee members for establishing a single program for industry.

The September 1991 Report to the President[7] advised that the NISP had been accepted by government and industry officials and the task force had successfully developed the critical components of the NISP. Supplemental standards were included for SCI, SAPs, and Energy/RD programs. The report advised that oversight organizations and responsibilities for the NISP would utilize existing offices, departments, and agencies and assign to them the responsibilities for the NISP, eliminating the need to create a new organization for oversight purposes. The concept of "minimum standards" for security had been abolished—stated standards would be the only standards. The report further stated that the responsibilities of the Secretaries of Defense and Energy, the NRC and the DCI, derived from their statutory and presidentially delegated authorities, had been preserved.

The report included a "critical path" for the next and succeeding phases which outlined significant events and important time-lines by which full implementation of the NISP could be realized by the end of 1995. The steering committee outlined the needed actions through 1995 and noted that the majority of other changes could be implemented by the end of 1993.

On 29 January 1992,[8] the President noted in a memorandum to the Secretary of Defense, "The government-industry task force you established has made considerable progress toward development of a single, coherent, and integrated program. This remarkably collaborative effort between government and industry will lead to significant improvements in the security of our Nation." The President continued, "I am especially pleased with the projected time frame in which you intend to fully implement this vital program, which will provide cost-effective and security development and delivery of systems essential to our national security."

Current Status

In June, 1992, a draft executive order (EO) establishing the NISP was sent to the National Security Council. The Office of Management and Budget (OMB) is completing coordination within the Executive branch. When signed, the current

[6] NISP Steering Committee Interagency Task Force Status Report on the NISP, 2 May 1991.

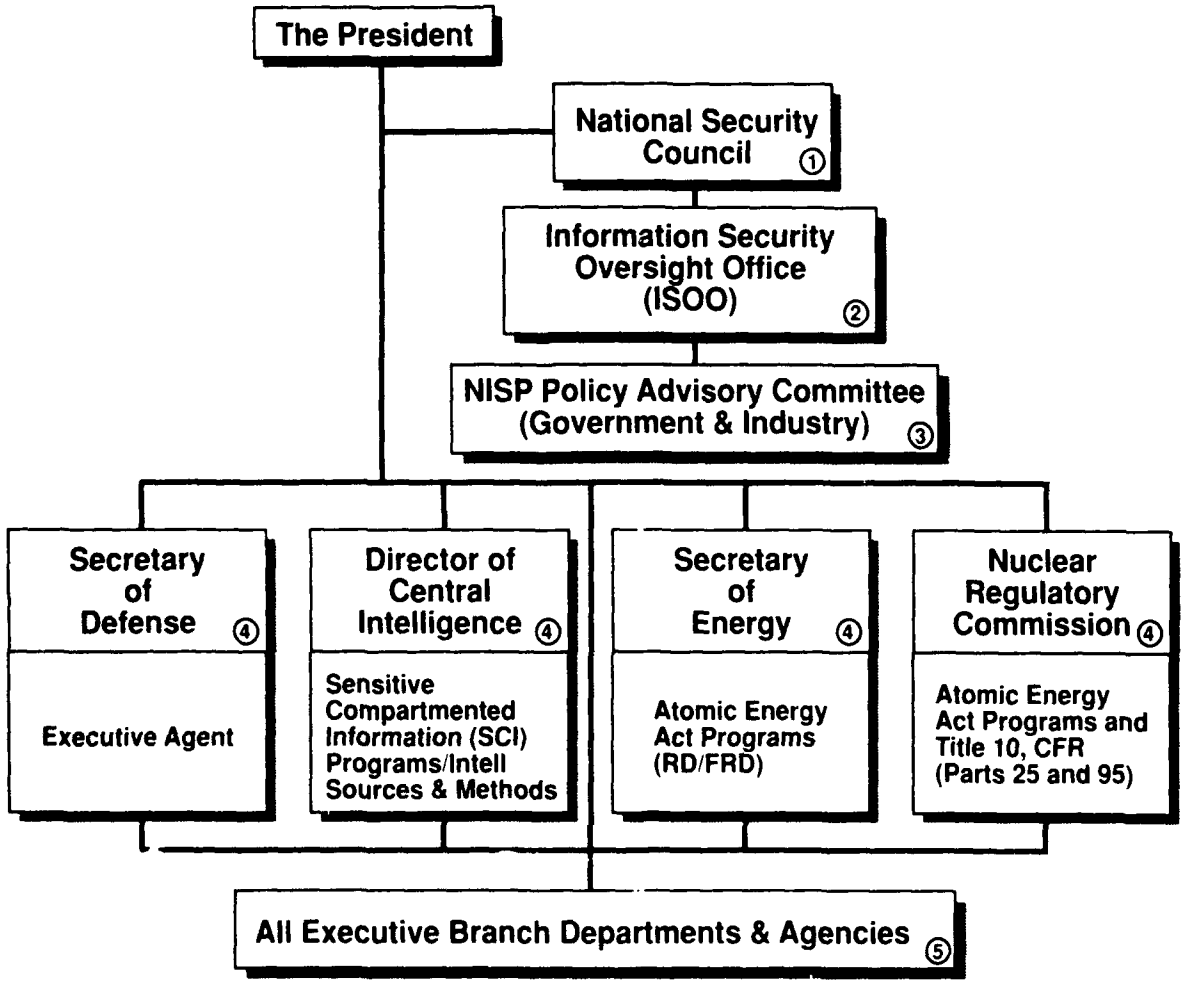
[7] The National Industrial Security Program—A Report to the President, September 1991.

[8] The President's Memorandum to the Secretary of Defense of 29 January 1992 on the National Industrial Security Program.

draft of the NISP EO calls for publication of the NISP Operating Manual within one year.

On June 17, 1992, the first draft of the National Industrial Security Program Operating Manual was forwarded to the other working groups by the Regulation Working Group for preliminary coordination and comment.

Figure 2. Proposed NISP Oversight Structure



1. Provide overall NISP policy direction
2. Oversee Executive Branch Department Agency actions to ensure compliance with the NISP subject to statutory or presidentially delegated authorities
   - Issue implementing directives
   - Provide guidance
   - Monitor and evaluate NISP compliance
   - Coordinate and recommend NISP policy changes
   - Review National Industrial Security Program Operating Manual (NISPOM) and agency regulations
   - Monitor NISP for improvements
   - Report annually on the NISP to the President
   - Chair NISPPAC
3. Advise on all matters concerning the policies of the NISP, including recommended changes and issues in dispute
4. Issue and maintain the NISPOM including special supplements
   Inspect and monitor contractor, licensees, and grantees
5. Implement the NISP

New DoDSI Correspondence Course

Basic Industrial Security for User Agency Personnel DS 2101

The Department of Defense Security Institute is proud to announce that its new correspondence course, Basic Industrial Security for User Agency Personnel (BISUAP), DS 2101, is available for enrollment. BISUAP will replace our resident Industrial Security Basic Course, which will no longer be offered.

BISUAP addresses the following topics:

- the Facility Security Clearance
- Personnel Security Clearances
- Visitor Control
- Classification Management
- Safeguarding Classified Information
- Automated Information Systems
- International Activities
- Violations and Compromises
- Inspections

Completion of Structures of Industrial Security (SIS), DS 2100, is strongly urged for those who will be taking BISUAP, DS 2101. Prior completion of both of these correspondence courses is mandatory for personnel who will attend the User Agency Inspector course at the DoDSI.

SIS covers patterns of organization prescribed by state laws to regulate commercial enterprises (business structures), procedures set up under federal laws to regulate governmental purchases (the defense acquisition cycle), and organizations formed under executive orders to promote national security (such as the Defense Industrial Security Program and the Defense Investigative Service).

BISUAP goes on to point out the basic requirements imposed on cleared defense contractors—and on the User Agencies—in the Industrial Security Manual for Safeguarding Classified Material (ISM), DoD 5220.22-M.

We've designed BISUAP for User Agency personnel who require a basic knowledge of industrial security, such as:

- Contracting officers and inspectors
- Security interns who require knowledge of industrial security
- Security specialists who are responsible for one aspect of security for a classified contract, such as personnel security, physical security, or information security.
- Personnel newly assigned to a special access program (SAP).
- Military personnel entering upon a 3-year assignment in the area of security.

Written as an orientation for User Agency personnel, BISUAP is also open to DIS Industrial Security Representatives and the Facility Security Officers in industry and members of their staffs. Enroll by submitting a DA Form 145 to the Army Institute for Professional Development (IPD) in Newport News, Virginia. DA Form 145 is available from cognizant security offices, DIS.

The Industrial Security Manual on computer diskettes

The ISM on Diskette.

Includes the full text of the 1991 ISM in ASCII format with an index (not found in the official hardcopy ISM), LIST — a search-and-retrieval software package, and a user's guide. This product is distributed in four 5.25" diskettes for IBM compatible systems by

FilmComm
641 North Avenue
Glendale Heights, IL 60139
Phone (708) 790-3300

The price of $17.50 includes all charges except postage. The first class postage charge is about $2.50. UPS and Federal Express are also available.

Automated SPPs and ISM.

Diskettes for either IBM compatible or Apple Macintosh systems are available from

National Security Institute
161 Worcester Road
Framingham, MA 01701
Phone (508) 872-8001

According to NSI, this is a complete on-line PC-based security library of current ISM requirements and company security procedures that you can custom tailor to fit your facility's security program. The package is designed for use with Microsoft Word or WordPerfect word processing packages and is available in 3.5" or 5.25" diskettes for $495.

SIMS On-Line ISM.

Includes the entire 1991 ISM with the latest issues of the Industrial Security Letter (ISL) also on magnetic media. The ISL, issued by the Defense Investigative Service, is an authoritative vehicle for guidance on ISM requirements. Included with these text files is a user's guide and "Golden Retriever," a versatile search and retrieval package which can be used to process other text files. Both IBM compatible and Macintosh versions are available. The entire package sells for $495 and can be purchased from

SIMS Software
Box 607
Solona Beach, CA 92075
Phone Tom Fleming at (619) 481-9292.

Intelligent Document™ ISM.

More than an on-line version of ISM, the Intelligent Document ISM offers quick solutions and instant answers; security officers can immediately "jump" to related sections, instantly find any word or phrase, and print all of the forms. Contains the complete 1991 ISM, cross-referenced with following Industrial Security Letters (ISLs). Also includes on-line expert guides, self-guided tours, and a word processor for notes. All future ISM revisions and the NISP Operating Manual are covered by a maintenance agreement.

Toyon Research
75 Aero Camino, Suite A
Goleta, CA 93117
Phone Kristine Shelly toll-free at 1-800-742-2334

Package sells for $395, including Reader's Guide and Technical Support.

You Can Host These Courses On-site at your Facility (Industry or Government)

Security Briefers Course (SBC) 5220.13, 2.5 days

Purpose: To improve your effectiveness as a security education briefer. You will receive instruction on how to:

- prepare a briefing plan;
- design and use briefing aids;
- present your briefings in a clear and interesting manner; and
- evaluate live briefings.

As the "Security" in the course title suggests, the briefings must address security requirements, but this is not the emphasis of the course. The course emphasis is on accomplishing the objectives listed above so that you become more skilled and more comfortable at speaking in front of others.

Train-the-Trainer Course (TTT) 5220.13a, 2 days

Purpose: To train you to teach the SBC. This workshop, conducted on the 2 days before a scheduled SBC, prepares you to be an instructor for the SBC. You will receive instruction by DoDSI staff on how to:

- use the SBC materials;
- present selected lessons in the SBC;
- facilitate the preparation of briefings;
- conduct practice briefing sessions; and
- evaluate live briefings.

Under DoDSI supervision, you will then spend the next 2.5 days teaching your first SBC.

If you are considering participating in the TTT, it is suggested that you: be responsible for your organization's security briefing program; be an experienced security briefer or a graduate of the SBC; have a need to train others to prepare and present security briefings; and have a working knowledge of security requirements. If you want to learn *how* to brief—choose the SBC.

To host the courses described above, please call Del Carrell, DoDSI at (804) 279-5314 or DSN 695-5314.

These courses are held in succession. The TTT precedes the SBC.

To host the SBC, you must be able to provide:

- ☐ one main classroom for 24 students
- ☐ 3 breakout rooms for 6 students each
- ☐ A-V equipment for all 4 rooms
  (Overhead projectors, screens, and writing surfaces for each room)
- ☐ At least two of the instructors and preferably more for the TTT.
- ☐ An on-site coordinator
- ☐ Invitations to other security organizations in your area in order to fill a class of 24.

The Department of Defense Security Institute (DoDSI) will:

- ✔ Provide the lead instructor and assume responsibility for the teaching success of the course.
- ✔ If necessary, provide security personnel from other organizations to help teach the course.
- ✔ Provide two full days of training for the instructors prior to starting the course.
- ✔ Provide the instructional materials in sufficient quantities for 24 students.
- ✔ Help the trainers teach the Security Briefers Course.

Security Briefers Course Dates and Locations

The following organizations are sponsoring the Security Briefers Course:

1 **September 23-25, 1992**

US ARMY - DPTMS
at Ft. Belvoir, VA
POC: Ms. Allison Troy (703) 805-2416, (DSN) 655-2416

2 **September 29-October 1, 1992**

JIGSAG (Joint Industry - Government Security Awareness Group)
at American Management Systems
1777 N. Kent Street, 14th floor
Arlington, VA 22209
POC: Ms. Susan Davis (703) 560-5000 x4778
Mr. Ron Thinnes (703) 556-6518

3 **October 28-30, 1992**

ISAC (Industrial Security Awareness Council) Salt Lake City
at Paramax Systems Corporation
640 North 2200 West
Salt Lake City, UT 84116-0225
POC: Mr. Joe Cotton (801) 594-5615

4 **November 4-6, 1992**

VSAC (Vandenberg Security Awareness Council)
at Vandenberg Air Force Base, CA
POC: Ms. Teresa Alarcio (805) 928-5711 x221

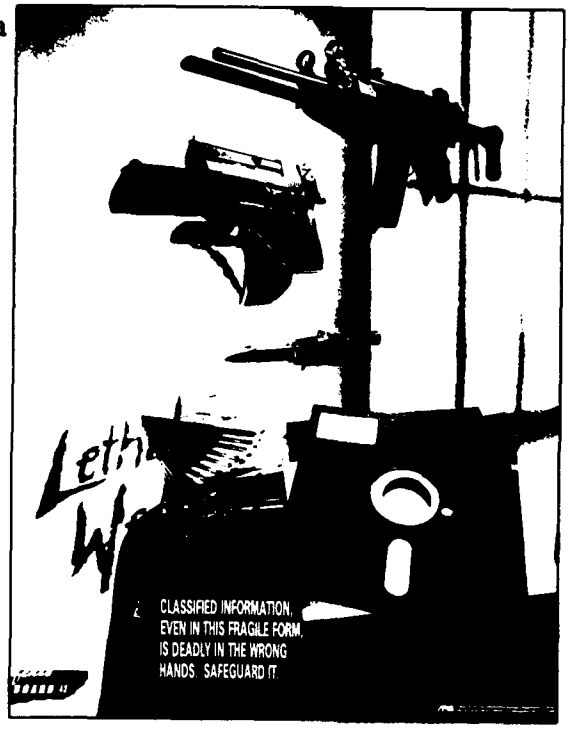
5 **April 28-30, 1993**

JIGSAG
at Center for Innovative Technology
Reston, VA
POC: Ms. Susan Davis (703) 560-5000 x 4778
Mr. Ron Thinnes (703) 556-6518

Please call the Point of Contact for course specifics and enrollment information.

Lethal Weapons Too

We have quantities of a computer security poster available for the asking. Originally produced by American Forces Information Service. Just call or write for your free copy. 17" x 22" color poster comes folded flat.



(804) 279-4223
Attn: EPD
DoD Security Institute
c/o DGSC
Richmond, VA 23297-5091

New Video . . .

National Industrial Security Program

BOEING

Date: 1992

Video #1	NISP Status	Date: March 1992	Length: 09:45
Video #2	NISP Overview	Date: February 1991	Length: 17:26
	NISP Status	Date: March 1992	

Cost per videotape: $17.50 for VHS $27.50 for 3/4"
(price includes shipping & handling)

Order from: FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

Summary: The Boeing Company has been involved in a national effort to replace the many redundant Government security programs levied on industry with one cohesive, integrated set of requirements. This program has become known as the National Industrial Security Program (NISP). Boeing, in support of the NISP, has produced two videos: an overview of the program and more recently an update status video.

DTIRP

The Defense Treaty Inspection Readiness Program and START Special Access Visits

By Mark Borsi
Chief, Special Actions Branch
Defense Investigative Service

Is your facility ready for a START treaty inspection? Before you get too alarmed, be advised that this applies only to a limited number of military and defense contractor facilities which might be subject to inspection under START or one of the other arms control treaties. In addition, the START itself is awaiting ratification by the Senate and of course will not be in effect until this happens.

But the writing on the wall is that at some point in the near future we must have in place appropriate security countermeasures at each "inspectable facility" in anticipation of a possible treaty inspection. The Defense On-Site Inspection Agency working with the Defense Investigative Service will play the leading role in assisting contractors to prepare themselves for such an inspection.

The DTIRP, design and purpose

According to its charter, *The Defense Treaty Inspection Readiness Program* (DTIRP) is a multidisciplined, all-source security vulnerability assessment program utilizing intelligence, counterintelligence, traditional security and operations security (OPSEC) methodologies. This essentially means that no boundaries are being drawn concerning where we obtain information about a potential threat and how we are going to counter that threat. The purpose of the DTIRP is to identify critical information and technology, assess vulnerability and recommend cost effective security countermeasures. The program was created to provide timely, informed recommendations to policy decision makers, program managers and facility managers in both government and industry. It is designed to foster awareness and ensure understanding, enabling everyone to appropriately prepare for the possibility of a treaty inspection.

A Multi-agency effort

The DTIRP employs technical and subject matter experts to provide objective analyses and recommendations to assist in the development of security countermeasures for each inspectable facility. On 25 June 1992 the Director, On-Site Inspection Agency was appointed as the Executive Agent for the DTIRP. Program policy direction is provided by the Deputy Assistant Secretary of Defense, Counterintelligence and Security Countermeasures. Participating agencies providing personnel and support include the Defense Investigative Service, the Defense Intelligence Agency, the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, the Community Counterintelligence and Security Countermeasures Office, and the Army, Navy and Air Force. The DTIRP's continuing mission is to assist the government and contractor community in providing counterintelligence and security countermeasures (CI&SCM) support in connection with inspection of U.S. facilities under arms control treaties.

Vulnerability assessments

The principal product of the DTIRP is a report (classified appropriately) focusing on arms control treaty specific vulnerabilities at inspectable sites. To date the DTIRP has conducted more than thirty assessments of START declared inspectable sites, both military and industrial. Initially developed in support of Strategic Arms Reduction Treaty (START) preparations, the DTIRP has expanded to provide support to all arms control treaties and agreements. Current examples include the Open Skies Treaty, the Chemical Weapons Treaty, and the Conventional Forces in Europe Treaty.

Special Access Visits

Arms control treaties include various "inspection regimes" or procedures established by the treaty involving foreign representatives inspecting U.S. facilities. In some cases, the U.S. knows in advance which facilities will be visited. In these cases, DTIRP studies are used to prepare the facility for an inspection. However some "regimes" allow for the inspection of "undeclared" facilities. The START Treaty has such a provision which is called a *Special Access Visit* (SAV). Essentially, the SAV provision was established to address the possibility of cheating by allowing a signatory to the treaty to challenge and inspect non-declared facilities. Fortunately, not all SAV requests will result in actual inspections. In fact, in these cases our objective is to resolve a challenge without allowing a visit at all. A U.S. Government response may be to (1) allow an inspection, (2) resolve a challenge by some alternative means, or (3) refuse to allow an inspection to take place.

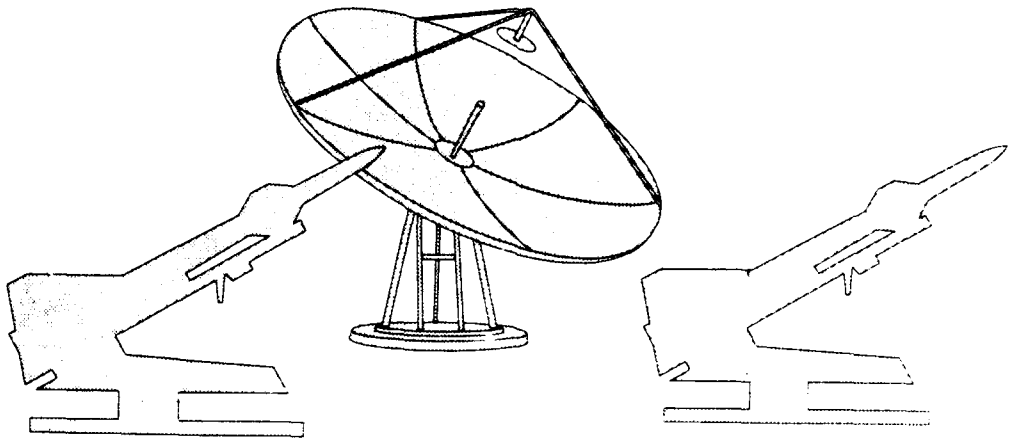
However, SAV challenges do create unique security concerns because the government has a very short time to determine the implications of allowing an intrusive inspection. To deal with these concerns the DTIRP is involved in START planning for Special Access Visits; developing databases which will allow us to perform statistical analyses and systematic tracking; and working to provide training, information, and assistance.

What is being done for inspectable facilities:

In addition to making vulnerability assessments, the DTIRP staff plans to evaluate facilities for vulnerability and likelihood of facing a SAV challenge, allowing the government to make sound and quick decisions when SAV requests occur. Security awareness is also an important part of the program. DTIRP will publish DIS Industrial Security Letter articles such as this one, and sponsor training for DIS Industrial Security Representatives. In fact, the person on the cutting edge for the DTIRP is the DIS representative in the field. Armed with training and an understanding of the arms control process, he or she will be able to provide information and assistance and to gather data to support DTIRP planning in the event a Special Access Visit is requested and approved. Knowledge, planning and timely preparation have proven keys to success in arms control treaty implementation in the past. The DTIRP is working to maintain the lead in assisting organizations in protecting their equities which are important to our national security.

What should you be doing now?

The information provided in this article is for the edification of security professionals in industry and government whose facilities may be subject to future treaty inspections. While no immediate action is required, it is not too early to start thinking about the security implications of these inspections. For more information on DTIRP activities you can contact the program manager: Chief, Office of Security, On-Site Inspection Agency, at 1-800-283-2179.



Security Penguin Contest

"Good job performance and lax security are poles apart."

By Art Fajans, formerly Director of Defense Security Programs
Office of Secretary of Defense

I hope you have had some fun with this. I know I have. The response was very positive. Over 90 entrees were submitted and that has made the selection of winners that more difficult. I like to think that everyone is a winner and that thoughtful approaches to effective security awareness that the contest may have engendered can be used locally at your activities, facilities, and organizations.

Not everyone is a fan of the security penguin, but I knew that before the contest was launched. One entry even suggested calling the penguin "STOOPID," but I was heartened by the fact that only three negative responses to the penguin were received.

This is one instance where I will not call for uniform implementation. The security penguin is not regulatory by any stretch of the imagination and whether you find it useful for your own programs or not, is entirely up to you.

Someone also sent me a copy of a USA Today article on penguins entitled, "Penguins are not as polite as their tuxedos might suggest." One quote from the article sums up my view of the penguin very well. "They are strong, tough, aggressive animals in a tough, harsh environment, and cute just does not apply." I can also relate to another definition of what a penguin represents—flippant dignity.

Trusty

A security professional's work holds particular importance to the environment in which that work is accomplished. Not only does that work strive to protect the organization's infrastructure, operations, activities, and systems, it must also be a good barometer of change. As a result of rapid and radical world geopolitical events including the break-up of the former Soviet Union and Warsaw Pact, security must be more flexible, efficient, and cost effective. We must recognize that changes in the threat as well as other challenging issues of affordability, risk, vulnerability and the value of information, systems, or technology will directly affect how security requirements will be defined and implemented in the future. To meet these challenges we will need security professionals who are strong, tough, aggressive people who can operate in a tough, harsh environment—cute just does not apply.

Another entry suggested that some of the slogan entries be shared so that the whole community might benefit from other ideas. Here are a few representative entries:

Think Security, Don't put US on thin ice
Security is a breeze, if you remember security A-B-C's
secURity—together we can do it!
Without your help—security will be out in the cold
Keep your cool-Security is the rule
The Cold War may be over but that's no reason to put a freeze on security
Don't let your secrets slip away
Avoid thin ice in your security program
Security violations melt my cool

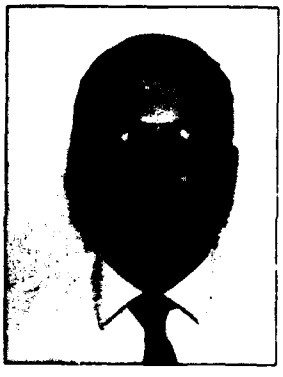
Security is like an iceberg, you only see the tip
World relations may be warming, but don't put security on ice
Security is a warm feeling
Security will never leave you in the cold
Keep your cool when handling classified information
Don't let security violations snowball—report them
Security is like a thermometer—let's PROTECT its degree by AWARENESS at all times
Spies and Traitors wind up in the cooler, don't skate on thin ice PROTECT OUR NATIONS SECRETS
Better button up your secrets
The cold war may be over, but without security—it could get very hot

AND NOW THE MOMENT OF TRUTH. The winners are:

For naming the penguin:

Trusty

David A. Davenport
Johnson Space Center
Houston, Texas



For the slogan:

Good Job Performance And Lax Security Are Poles Apart

D. Wilmer Rivers, Jr.
Teledyne Geotech
Alexandria, Virginia

Security Penguin — The Final Chapter?

The preceding article by Art Fajans provides some insight into Art's thinking when he originated the idea of a security logo or mascot in the form of a penguin and sponsored a contest to name the bird and come up with a slogan. Needless to say, Art got a lot of good-natured ribbing from all quarters on his "penguin thing," which culminated with his retirement in April 1992.

At his retirement luncheon he was presented with a lot of penguin memorabilia, including an item depicted in the accompanying photo. Appropriately, the final presentation was a rendering of Trusty's tombstone, with an appropriate epitaph.

Art denied the "passing" of Trusty and adamantly asserted his continued existence. And he may be right. While "Trusty" does not exist as an "official" logo, it's just possible that reported sightings of the friendly bird (like Elvis) may surface from time to time in the future.

Time will tell . . .

For those of you who wish to adopt Trusty to promote your security programs, please ask us for the artwork and we will provide you with a copy.

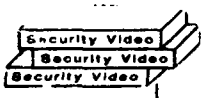
A Clearinghouse for Security Education Products

A couple of Bulletins ago we ran the following announcement and got a good response. We're running it again in case we missed you the first time.

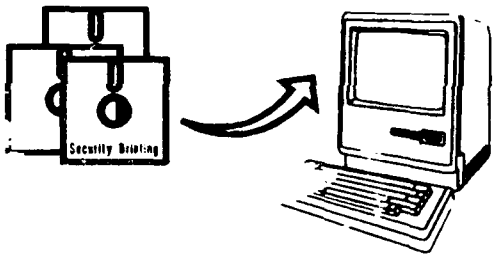
When it's time for you to give a security briefing, does the availability of training materials remind you of Mother Hubbard's cupboard? When presenting security briefings, have you ever felt that you and the flight attendant addressing a plane full of frequent flyers have a lot in common? Whether you are a security novice and know no sources for security education materials or a security expert but know only the same old sources, a Security Education Project is underway in an effort to help.

The Joint Industry/Government Security Awareness Group (JIGSAG) is supporting the Department of Defense Security Institute's efforts in setting up a clearinghouse for security education materials. The idea is to have a central point to send products that have proven themselves effective—in other words, that your audience likes—so that, with everyone sharing products, you suddenly have a tremendous pool of resources to draw from.

The products initially targeted for collection are *videotapes* and *PC-based tutorials/briefings.* The members of the Project encourage your participation and ask that you forward your product to:



Ronald Thinnes
Attn: JIGSAG Video Review
BTG, Inc.
1945 Old Gallows Rd.
Vienna, VA 22182
(703) 761-6517
fax: (703) 556-9290



All products will be evaluated by JIGSAG for accuracy, quality, propriety in accordance with defined standards, and applicability within the DOD/Industrial Security communities. The committee will also send a description of *every* product to the DODSI along with the evaluation results. An example is provided on the next page. DODSI will have the best ones reproduced and distributed either through the DIS Education and Training Specialists (for loan) or through inexpensive commercial distribution centers (for purchase—$20-30). DODSI will also publish a catalog of *all* submitted training materials, similar to what is provided in its "Training Aids for Security Education."

Don't be reticent. Even if your video hasn't won an Oscar, it's a "go" for entry in the catalog and may be a good candidate for distribution. Why don't you take a minute to rummage through your cabinets for any training products you've put together. They don't have to be stellar acts—their novelty and availability are important factors, too.

With your help, this could turn out to be a great success!

Product Profile

Product Name: ..... Jonathan Pollard—A Portrayal
Product Type: ..... Videotape
Subject Focus: ..... Espionage
Production date: 1991
Produced by: ..... Defense Intelligence Agency
Classification/Limitations: ..... Unclassified
Availability data: ..... copies available from FilmComm
Charge for copies: ..... approx. $20-30 depending on tape size and mode of delivery

Videotape Data

format: ..... 1/2" or 3/4" Running Time: 18:00

General Assessment

Applicability: ..... suitable for all
Propriety: ..... no propriety problems noted
Technical accuracy: ..... generally accurate
Geographic limitations: ..... not geographically limited
Currency and durability: ..... current and having an indefinite life-span
Production quality: ..... high quality production
Interest: ..... able to hold attention well
Strength and clarity of message: . the message is strong and clear
Tone and impression: ..... generally positive and constructive
Use of time: ..... length and pacing are on target
Flexibility: ..... could be tailored easily
Prerequisite knowledge: ..... minor presumptions about knowledge
Orientation: ..... suitable for all audiences
Credibility: ..... high degree of realism and credibility

Description and Evaluation:

Jonathan Pollard was an employee of the Navy, but because of his position as a counterintelligence analyst, he had access to hundreds of classified documents from the intelligence departments of many federal agencies—and at the time of his arrest, had stuffed enough of these documents in his apartment to fill a space 10' x 6' x 4'. Pollard is an American who spied for Israel. He is serving a life sentence for his espionage work. And the reason he is, is thanks in part to an observant co-worker who noticed suspicious activity and was smart enough to report it. This video reenacts the events at Naval Intelligence Command in Suitland, Maryland, that led to the realization Pollard was involved in more than just doing his job.

A New Crowd Pleaser at DoDSI!

The first **Advanced Industrial Security Management Course** (AISMC) will be taught at the DoD Security Institute from November 17-19, 1992, in Richmond, Virginia. This course for defense contractor personnel goes beyond the ever-popular Industrial Security Management Course to emphasize specific requirements and administrative procedures in safeguarding classified defense information at possessing facilities.

Some of the topics to be presented:

- International Aspects
- Independent Research and Development
- STU-III
- Programmatic Inspections
- AIS Security
- Alarms
- Technology Transfer

Assisting the DoDSI faculty will be Department of Defense specialists offering unique insight into particular programs.

This first AISMC class is by invitation only, including many attendees who, we hope, will provide us comment and feedback with an eye toward making the course more usable. Consequently, there are no vacancies in the November course. However, we encourage you to sign up for one of the dates offered below during FY 93:

March 30 - April 1, 1993
June 15 - 17, 1993
August 31 - September 2, 1993

The prerequisites. To attend the AISMC you:

- ✔ must have been involved with the Defense Industrial Security Program for at least three years.
- ✔ must have successfully completed the *Essentials of Industrial Security Management* and *Protecting Secret and Confidential Documents* independent study courses.
- ✔ should also have successfully completed the Industrial Security Management Course.

For additional information about registering, please call the DoDSI Registrar's Office at (804) 279-4891.

SPIN

Security Program Improvement Network

Made improvements to your security program? Added some nifty features to help you meet your security requirements better or with less resources? Want to know what others have done, are doing or thinking about that you could use to do a better security job?

You're in luck. DoD has set up a program to capture and share that information. It's called the *Security Program Improvement Network,* a long enough title for us to call it "SPIN" for short.

WHY SPIN

The security pros in DoD and its contractors and our counterintelligence folks know that getting the security job done right is more than just doing what you have to do. And, if one of them has found a better way, you can bet that there are plenty of others who would want to adopt it. SPIN is the link between those with tried and effective solutions and those still looking for them.

By bringing the two together, one's success becomes success for all. If we really get good at sharing these solutions, think what it will mean for the strength of our security programs and the wise use of our security resources.

But SPIN's not just limited to the pros. DoD has that whole range of cleared people in its activities and contractors who work under our security programs day-in and day-out. They've been a continuing source of good ideas that have led to improving what we do in security. After all, they're the people who have the most influence on whether security does or doesn't work.

WHAT'S SPIN AFTER

Since its purpose is to "spread the word" on how we can improve what we do in security implementation, SPIN is looking for successes or solid ideas on making improvements. It's after the small improvements in day-to-day operations as well as the "super-colossal" changes and everything in-between. (Don't keep the small improvements to yourself! When you multiply those times the number of locations that could use them, the benefits can rival or exceed the value of the "super-colossal.") SPIN wants to know about:

- Successes in getting better results in applying our security program requirements that others can try. Those may come from greater effectiveness or resource savings while still meeting the requirements. They should be ones that have a wide application in your component, within DoD or among DoD contractors. They may be in:
  - » how you operate the programs, the procedures you have introduced, the way you have organized, what you have done to motivate security support;
  - » your approach to assistance and inspection, how you've established the value of security, how you've handled continuous evaluation of cleared personnel,
  - » the equipment you use, the software you have created or applied, how you've overcome a problem inherent in the requirements, etc.
- Ideas on making improvements you've been thinking about in meeting the security requirements. SPIN can get you some feedback from others who may have already implemented or tried those ideas or might help you bring them about.
- Articles, books, other publications, or software you have found particularly helpful in improving your security operation.

SPIN is concerned with doing better what we are asked to do rather than with changes in program requirements. That's not because it discourages change; it's just that we need to keep it focused to get the most benefit from it. (The Institute hopes to begin a separate publication that will give you a way to share your thoughts on program changes.)

HOW SPIN WORKS

SPIN Coordinator and Committee

DoDSI's SPIN Coordinator will receive your submissions, refer them as needed for review by volunteer SPIN committee members from DoD and DoD's contractors, work with you to prepare them for publication, and make sure you are recognized for your participation.

The SPIN committee will aid the Coordinator in selecting submissions for publication and for special recognition and in deciding added information that would be useful.

Publication

Selected submissions will appear in the DoDSI *Security Awareness Bulletin*. As the number warrants, we'll look to publishing special editions of the *Bulletin* on SPIN or to producing a separate SPIN publication.

DoDSI will separately publish submissions that have restricted dissemination. We're also exploring having SPIN as well as DoDSI and other material available to you on an electronic bulletin board. (More on that in a subsequent *Security Awareness Bulletin*).

Periodically, we'll put together the other submissions for separate distribution as a "grab bag" of ideas and actions that may help. For materials that may be generally useful, we'll announce how copies can be obtained.

Recognition

Besides the good feeling from sharing your successes and ideas with others and knowing you're helping improve security, SPIN wants to give you special recognition. After all, it's your time and effort!

So, look for a Certificate of SPIN Participation that we'll send to each submitter. That will come through your command or company commending you for the contribution unless you tell us you'd prefer to receive it directly.

Formally published submissions will identify the submitters in the byline unless anonymity has been requested. The SPIN Coordinator and Committee will review those each year to select the ones they recommend for special recognition. They'll refer them to the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures) for a personal thanks for the contribution and a special certificate. We'll also announce the top Spinners in the *Bulletin*.

TAKING PART

How do you share your successes and ideas in doing the security job better? It's quite easy.

- For your successes, just describe the problem or situation involved, what you did to make the improvements, how you did it, what difficulties you had, if any, in doing it and how you overcame them.

- For ideas you want to "test" with others, just relate what it is, why you think it will help, and how it would work.

- For publications and software, send your description of their value and application. If you don't include them, you'll need to say where they can be obtained and identify the author, title, etc. If you send software, include a brief description of what it does, how to use it, and any conditions for its release to others.

- Be as detailed as need be and include a cite of any related regulation portions that apply.

- If your submission is classified, limit it to no higher than Secret and make sure you've got it correctly portion marked.

- Submit your contribution in typed form and, if you can, include a copy on floppy diskette (5.25 or 3.5 inches) in a DOS program. Make sure you:

  » Include your name, organization, component or company, mailing address, and telephone number (commercial and, where available, DSN numbers).

- Tell us if you want your name, organization or component or company identified in reviewing or publishing your contribution.
- Include any restrictions that you know of and the authority on releasing its content to other federal agencies and personnel, to contractors, or to the public.

Send them to:

DoD Security Institute
ATTN: SMD(SPIN Coordinator)
c/o DGSC
8000 Jeff Davis Highway
Richmond, VA 23297-5091

For assistance or more information, contact the SPIN Coordinator, Carl Roper, at the above address or by telephone at (804) 279-5593 or DSN 695-5593. Carl has the DoDSI flyer on SPIN which he can send to you.

Put out the word to your organizations and personnel and encourage their participation. SPIN starts the moment we have the first submission. Join in now!

New Videos . . .

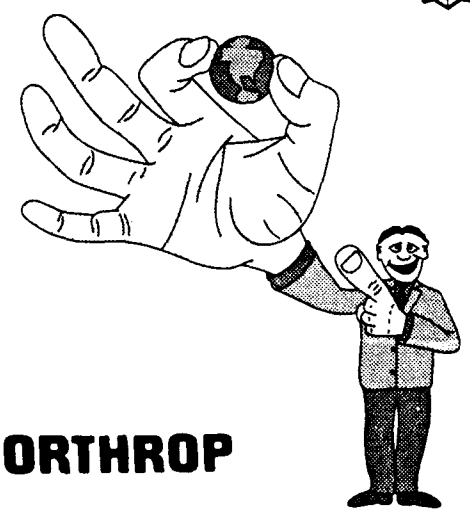
Briefing the Susceptible Traveler

NORTHROP

Date: 1991 Length: 11:44 min. Medium: 1/2"

Order from: Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178

Summary: A brief-the-briefer video for security managers who need to brief employees traveling outside the U.S. Produced by Northrop Corporation in conjunction with the FBI's Susceptible Traveler Program. Closed captioned for the hearing impaired.



Foreign Travel Briefing — Don't Leave Home Without It

NORTHROP

Date: 1991 Length: 7:10 min. Medium: 1/2"

Order from: Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178

Summary: Designed to be viewed by the average employee traveling to a foreign country. Produced by Northrop Corporation. Closed captioned for the hearing impaired.

ANNOUNCING...

Basic Personnel Security Investigations
Resident Course

In response to requests for training in basic personnel security investigations from various security organizations, the DoDSI will offer a two-week basic PSI Course in FY 1993 to be held at DoDSI, Richmond, VA.

January 25 - February 5, 1993

To be eligible for attendance at this course, you must be a Federal employee performing in a security-related function, e.g. investigator, investigative technician, personnel security specialists, etc. The course covers general aspects of personnel security investigations. The first week of the course addresses various procedures and techniques for record reviews and interviews, development and resolution of security issues and fundamental report writing. Attendees participate in several practical exercises to use their interviewing and record reviewing skills. The second week of the course is designed for those individuals that are responsible for also conducting various types of subject interviews in personnel security. Emphasis is placed on learning skills in subject interviewing through a series of practical and criteria exercises. Individuals that do not conduct subject interviews may elect to attend only the first week of this course. The second week is limited to those who are required to conduct Subject Interviews as part of their job. You should indicate which learning track is appropriate for you when applying for attendance.

Fill out the attached form and mail it to the Registrar's Office at the Department of Defense Security Institute, c/o DGSC, 8000 Jefferson Davis Highway, Richmond, VA 23297-5091. For course information, call the Personnel Security Investigations Department (804) 279-4179 or AVN 695-4179.

Complete, detach and return

please print — MAIL TO: Registrar, DoDefense Security Institute, 8000 Jeff Davis Hwy., Richmond,VA 23297-5091

Your Name _____

Title _____ _____

SSN _____

Agency Name _____

Address _____

_____

_____

Telephone _____

Supervisor _____

Course Title Basic Personnel Security Investigations

Course Dates First Week Only: ❑ _____ Two Weeks: ❑ _____

Industrial Security — Customized

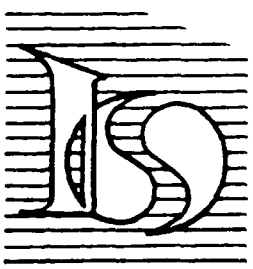
To help both you and the already overworked Industrial Security Rep, the Industrial Security Department faculty at DoDSI now has a one- to two-day training session (for government and industry) that covers industrial security subjects *you* can tailor to your specific needs. For example, do you have numerous Document Control personnel who need training in accountability, reproduction, destruction? We can help. *You* work with us in the design. *You* pick the site; no cost other than travel, food, and lodging for one or two instructors.

For more details about this offer, please call either Wayne Lund or Michael Black at (804) 279-5257 (DSN 695-5257).

New Videos . . .

The Interagency OPSEC Support Staff has just released two new videotapes to the OPSEC community. The tapes had their "world premier" at the National OPSEC Conference.. Videos are no cost.

Order from: IOSS
Attn: Publications Department
6411 Ivy Lane Ste 400
Greenbelt, MD 20770-1405



Applying OPSEC in R&D Activity

Date: 1992 Length: 16 min.

Summary: Discusses the role of OPSEC in protecting sensitive information, especially at test ranges. It is an edited version of a briefing originally presented to the Strategic Defense Initiative Organization.

OPSEC: Protecting Our Edge

Date: 1992 Length: 9 min.

Summary: Explains how OPSEC can help protect sensitive technological and economic information from loss to foreign competitors. Produced by the Defense Information Systems Agency.

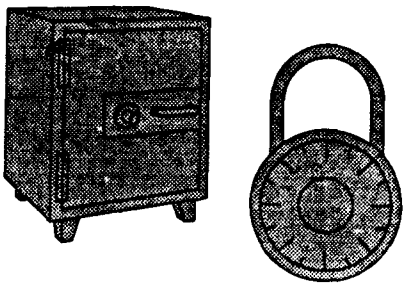
New Video . . .

Safes, Locks, and Videotapes

Date: 1991 Length: 12 min. Medium: VC 1/2" or 3/4"

Order from: FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

or Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178



Summary: This video talks about the different GSA containers and locks; container labels, how to inspect a container and lock. How to change a combination. Lists security device manufacturers. Comes with pamphlet that provides additional information. Produced by the Defense Security Institute.

New Video . . .

Friend and/or Foe, The New Espionage Challenge

HUGHES

Date: 1991 Length: 20 min. Medium:VC

Order from: Pro Star International
P.O. Box 21526
Salt Lake City, UT
1-800-775-0761
fax: (801) 943-5178

or FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

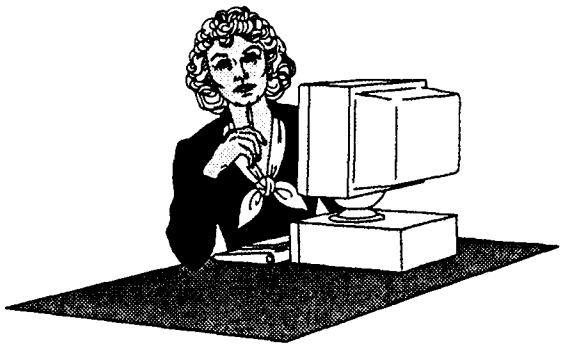
Summary: An up-to-date film on the changing threat to national security showing that our international friends are sometimes our foes. When any country's need or desire for our technology spurs them to illegally acquire non-exportable U.S. technology, it has passed from friend to adversary. And attempts are being made all the time. The cooperation among U.S. Customs, American industry, and the FBI is helping to curb the increasing flow of illegal export. This 20-minute film clearly states the enormity of the problem and what you can do to help prevent further loss of our nation's top security priority: its competitive edge in world technology. Produced by Hughes Corporation in cooperation with the FBI and U.S. Customs. Pro Star International also has a closed captioned version for the hearing impaired.

New Video . . .

Is Your PC Data Safe?

Date: 1992 Length: 21 min. Cost: $325.00
15-day preview fee: $27.50 (includes shipping/handling)

Order from: Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178



Summary: This computer security training program for government contractors comes with a 21-minute video, instructor's manual, and student guide materials. Video shows the importance of following the guidelines in Section 8 of the Industrial Security Manual, and your SPP. Dramatization tells the story of a new company president with a poor security posture and the tips he receives from his ghostly colleague. Video is closed captioned for hearing impaired. Produced by Pro Star International. Program also comes in a second version: protecting trade secrets and proprietary information.

Deliver!

The Security Management Department at the DoD Security Institute has written an easy-to-follow pamphlet called Deliver! that answers your questions on transmitting and transporting classified materials. To order, see form on last page of this Bulletin.

Security Awareness Publications Available From The Institute

Postage Requirement: We ask that you provide postage, but the publications are free of charge. Instructions for figuring postage are provided on the next page. See ordering instructions below.

To Order:

1. Check publications on the list below.
2. Add total weight. Include 1 oz. for envelope.
3. Figure the postage using information on the next page.
4. Choose envelope size (see chart 4, next page); affix postage and mailing label.
5. Send this page with **stamped** (no checks, please), self-addressed envelope to:

DoD Security Institute
Attn: EPD
c/o DGSC
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

(TAS) Training Aids for Security Education. June 1992. Catalog of audiovisual and printed material of interest to security educators. Instructions for ordering. . . . ___ 3.5 oz.

(REC) Recent Espionage Cases: Summaries and Sources. September 1991. Seventy-eight cases, 1975 through 1989. "Thumb-nail" summaries and open-source citations. . . . ___ 3.5 oz.

(FIT) The Foreign Intelligence Threat to U.S. Defense Industry. By Defense Security Institute staff. January 1991. . . . ___ 3.0 oz.

(FTB) Foreign Travel Briefing. 1981. Script of briefing designed for cleared employees traveling to designated countries. Outlines methods used by hostile intelligence services and precautions against them. (For 14-minute tape/slide briefing, see "Training Aids for Security Education.") . . . ___ 2.5 oz.

(SIT) Soviet Intelligence Targeting of the US Scientific Community, August 1990. A basic tutorial for those in contact with the Soviet scientific community. . . . ___ 3.0 oz.

(CUT) Control of Unclassified Technical Data with Military or Space Application, May 1985. DoD 5230.25-PH. 20-page booklet prepared by the Office of Secretary of Defense explaining the DoD program to limit public disclosure of export-controlled technical data and the special markings for technical documents. . . . ___ 1.5 oz.

(SAM) Soviet Acquisition of Militarily Significant Western Technology: An Update, September 1985. Western products and technology secrets are being systematically acquired by intricately organized, highly effective collection programs. . . . ___ 5.5 oz.

DELIVER! A pamphlet on how to transmit and transport your classified materials. . . . ___ 1.0 oz.

Individual back issues of the *Security Awareness Bulletin* up through #2-89 are no longer available from the Institute. Reprints of past feature articles have been brought together under a single cover in a publication, *Security Awareness in the 1980s*. Available from the Government Printing Office, stock number 008-047-00394-3. Price is $11.00. To order call (202) 783-3238.

Security Awareness Bulletin. Back issues available from the Institute:

(1-90)	Oct 89	Foreign Travel. FOR OFFICIAL USE ONLY. . . .	___ 3.0 oz.
(2-90)	Jan 90	The Case of Randy Miles Jeffries . . .	___ 3.0 oz.
(3-90)	Apr 90	Beyond Compliance – Achieving Excellence in Industrial Security . . .	___ 5.5 oz.
(4-90)	Aug 90	Foreign Intelligence Threat for the 1990s . . .	___ 3.5 oz.
(1-91)	Jan 91	Regional Cooperation for Security Education . . .	___ 3.5 oz.
(2-91)	Sep 91	AIS Security . . .	___ 3.5 oz.
(1-92)	Oct 91	Economic Espionage . . .	___ 3.5 oz.
(2-92)	Feb 92	Self-Inspection Handbook . . .	___ 4.0 oz.
(3-92)	Mar 92	OPSEC . . .	___ 2.5 oz.
		Allow for envelope . . .	✓ 1.0 oz.
		Total weight . . .	____
		Send postage in the amount of . . .	$_____

Postage Information

If total weight is **11 ounces or less**:

Chart 1: find the amount of postage

Example: If total weight is 4.5 oz., postage is $1.21.

Chart 1

Weight not exceeding:	First Class Rate
1 oz.	$0.29
2 oz.	0.52
3 oz.	0.75
4 oz.	0.98
5 oz.	1.21
6 oz.	1.44
7 oz.	1.67
8 oz.	1.90
9 oz.	2.13
10 oz.	2.36
11 oz.	2.59

Chart 4 Envelope Size

Publications measure 8 1/2 x 11"

No. of pubs	envelope
1-9	9 1/2 x 12"
10-18	10 x 15"

If total weight is **greater than 11 ounces**:

Chart 2: find postal zone using first 3 digits of your ZIP code

Chart 3: determine amount of postage using weight and zone

Chart 2 Postal Zone Chart

ZIP Code Prefixes	Zone	ZIP Code Prefixes	Zone	ZIP Code Prefixes	Zone
004-005	3	295	3	513-560	5
006-009	7	296	4	561-576	6
010-043	4	297	3	577	7
044	5	298-322	4	580-585	6
045	4	323-325	5	586	7
046-047	5	326	4	587	6
048-065	4	327-349	5	588-593	7
066	3	350-353	4	594	8
067	4	354-355	5	595	7
068-119	3	356-359	4	596-599	8
120-126	4	360-361	5	600-608	5
127	3	362	4	609	4
128-147	4	363-367	5	610-617	5
148-163	3	368	4	618-619	4
164-165	4	369	5	620-667	5
166-172	3	370-374	4	668-672	6
173-174	2	375	5	673	5
175-196	3	376	3	674-693	6
197-223	2	377-379	4	700-705	5
224-225	1	380-383	5	706	6
226	2	384-385	4	707-729	5
227	1	386-397	5	730-742	6
228-229	2	399-410	4	743-744	5
230-232	1	411-412	3	745-748	6
233-237	2	413-414	4	749	5
238-239	1	415-416	3	750-754	6
240-241	2	417-418	4	755	5
242-243	3	420	5	756-784	6
244-245	2	421-436	4	785	7
246-253	3	437-439	3	786-796	6
254	2	440-443	4	797-831	7
255-266	3	444-447	3	832-844	8
267-268	2	448-455	4	845	7
270-274	3	456-457	3	846-864	8
275-279	2	458-496	4	865-885	7
280-286	3	497-509	5	889-999	8
287-294	4	510-512	6		

Chart 3 Priority Mailing Rates by Zone

Weight, up to --	*1, 2, 3*	*4*	*5*	*6*	*7*	*8*
2 lbs	$2 90	$2 90	$2 90	$2 90	$2 90	$2 90
3 lbs	4 10	4 10	4 10	4 10	4 10	4 10
4 lbs	4 65	4 65	4 65	4 65	4 65	4 65